II. (U) THE UNITED STATES HAS PROPERLY ASSERTED THE STATE SECRETS PRIVILEGE IN THIS CASE.

(U) The United States has properly asserted the state secrets privilege in this case. The Director of National Intelligence, J. Michael McConnell, who bears statutory authority as head of the United States Intelligence Community to protect intelligence sources and methods, *see* 50 U.S.C. § 403-1(i)(l),[14] has formally asserted the state secrets privilege after personal consideration of the matter. *See Reynolds,* 345 U.S. at 7-8. DNI McConnell has submitted an unclassified declaration and an *in camera, ex parte* classified declaration, both of which state that the disclosure of the intelligence information, sources, and methods described therein would cause exceptionally grave harm to the national security of the United States. See Public and *In Camera* Declarations of J. Michael McConnell, Director of National Intelligence. Based on this assertion of privilege by the head of the United States Intelligence Community, the Government's claim of privilege has been properly lodged.

(U) As set forth in the following section, the information at issue in the Government's privilege assertion is central to the resolution of this case and the harms to national security that would result from its disclosure require dismissal of the action.

III. (U) INFORMATION SUBJECT TO THE STATE SECRETS PRIVILEGE IS NECESSARY TO ADJUDICATE PLAINTIFFS' CLAIMS AND, THUS, THIS ACTION CANNOT PROCEED.

(U) As noted above, once the state secrets privilege is asserted, the Court must evaluate the consequences of that assertion on the case. Here, state secrets are "so central to the subject matter of the litigation that any attempt to proceed will threaten disclosure of the privileged matters." *Fitzgerald*, 776 F.2d at 1241-42. Indeed, Plaintiffs' cannot prove their standing or claims, and Defendants cannot present a full defense, without the privileged information. *See*

---

[14] (U) See 50 U.S.C. § 401a(4) (including the National Security Agency in the United States "Intelligence Community").

Kasza, 133 F.3d at 1166. Specifically, adjudicating each of Plaintiffs' claims would necessarily require: (1) confirming or denying the existence of a NSA-Verizon relationship with respect to the particular alleged activities; (2) confirming or denying that the named Plaintiffs have been subject to any alleged activities; (3) proving that the content surveillance program authorized by the President after 9/11 was not a dragnet of domestic communications as alleged; (4) confirming or denying the existence of the alleged communications records activities; and (5) disclosing the nature and scope of any such alleged activities, including the precise nature of the activities, how they were conducted, why they were conducted, when they were conducted and for how long, and the intelligence value of the activities. Because such information cannot be disclosed without causing exceptionally grave damage to the national security, every step in this case—either for Plaintiffs to prove their claims, for Defendants to defend them, or for the United States to represent its interests—runs into privileged information.

A. (U) Whether or Not MCI/Verizon Has a Relationship with the NSA is a State Secret Necessary to Decide This Case.

(U) The first and most obvious matter at issue is whether MCI and Verizon have assisted the NSA in any alleged intelligence activities at issue. A confirmation or denial of the alleged relationship, however, is precluded by long-standing authority, not only under the state secrets privilege, but under the *Totten* doctrine as well. These are closely related but distinct grounds for dismissing Plaintiffs' claims.

1. (U) The *Totten* Doctrine Requires Dismissal of this Action to Protect Whether or Not MCI/Verizon Has a Relationship with the NSA.

(U) In the first instance, this case squarely falls within the *Totten/Tenet* rule of dismissal. In *Totten v. United States*, the Supreme Court held that public policy forbade a self-styled Civil War spy from suing the United States to enforce an alleged secret espionage agreement. In rejecting the claim of the alleged spy's estate that the United States had refused to pay him under a contract he allegedly entered into with President Lincoln to spy on Confederate military operations, the Supreme Court held that "[t]he service stipulated by the contract was a secret service; the information sought was to be obtained clandestinely, and was to be communicated privately; the employment and the service were to be equally concealed." *Totten*, 92 U.S. at 107. The Court added:

> Both employer and agent must have understood that the lips of the other were to be forever sealed respecting the relation of either to the matter. This condition of the engagement was implied from the nature of the employment, and is implied in all secret employments of the Government in time of war, or upon matters affecting our foreign relations, where a disclosure of the service might compromise or embarrass our Government in its public duties, or endanger the person or injure the character of the agent.

Id. For this reason, the Court held that "public policy forbids the maintenance of any suit in a court of justice, the trial of which would inevitably lead to the disclosure of matters which the law itself regards as confidential, and respecting which it will not allow the confidence to be violated." *Id.*

(U) This precise principle was reaffirmed by the Supreme Court in *Tenet v. Doe*. In *Tenet*, alleged former spies sued the United States and the Director of the Central Intelligence Agency (CIA) claiming that the Government had failed to provide the assistance it had promised in return for their espionage services. *See* 544 U.S. at 3-5. The Supreme Court held that the Court of Appeals was "quite wrong" in holding that *Totten* was limited to a mere "contract rule" prohibiting breach-of-contract claims seeking to enforce the terms of espionage agreements but not barring other claims based on due process or estoppel theories. *Id.* at 9. Instead, the Court reiterated that "'public policy forbids the maintenance of *any* suit . . . which would inevitably lead to the disclosure of [confidential] matters.'" *Id.* (quoting *Totten*, 92 U.S. at 107) (emphasis added). The Court thus held that "*Totten* precludes judicial review in cases such as respondents' where success depends upon the existence of their secret espionage relationship with the Government." *Id.*

(U) Indeed, the *Tenet* Court went on to note that the *Totten* rule was not merely an "early expression" of the state secrets evidentiary privilege under *Reynolds*, but a "categorical bar" to such claims. Specifically distinguishing the privilege, the Court held that *Reynolds* "in no way signaled our retreat from *Totten's* broader holding that lawsuits premised on alleged espionage agreements are altogether forbidden." Id.[15] Noting that "[e]ven a small chance that some court will order disclosure of a source's identity could well impair intelligence gathering and cause sources to 'close up like a clam,'" *Tenet*, 544 U.S. at 11 (quoting *CIA v. Sims,* 471 U.S. 159, 175 (1985)), the Court concluded that the "possibility that a suit may proceed and an espionage relationship may be revealed, if the state secrets privilege is found not to apply, is unacceptable." *Id.*

(U) In this case, the sum and substance of Plaintiffs' allegations are that MCI and Verizon have "a secret espionage relationship with the Government." *Totten*, 92 U.S. at 107. An adjudication of Plaintiffs' claims would necessarily require either confirming or denying the existence of that relationship. Accordingly, dismissal of this action is required by the *Totten/Tenet* categorical bar to litigation that threatens to disclose alleged covert relationships. The *Hepting* decision recognizes that a case such as this "involves an alleged covert relationship" between the Government and telecommunications carrier, but the Court nevertheless held that *Totten* and *Tenet* pose no bar for two reasons. First the Court held that *Totten* is limited to claims seeking to enforce an espionage relationships. Second, the Court found that AT&T and the Government had already effectively admitted the relationship. Neither conclusion should apply here.

---

[15] **(U)** The *Tenet* Court observed that *Reynolds* itself refutes this very suggestion because *Reynolds* cites *Totten* as a case "where the very subject matter of the action, a contract to perform espionage, was a matter of state secret," and declares that such a case was to be "dismissed on the pleadings without ever reaching the question of evidence, since it was so obvious that the action should never prevail over the privilege." *Reynolds*, 345 U.S. at 11 (emphasis added).

(U) As to the scope of *Totten*, the Court held that "[t]he implicit notion in *Totten* was one of equitable estoppel: one who agrees to conduct covert operations impliedly agrees not to reveal the agreement even if the agreement is breached." *Hepting*, 439 F. Supp. 2d at 991. In the Court's view, because "AT&T, the alleged spy, is not the plaintiff here," plaintiffs have "made no agreement with the government and are not bound by any implied covenant of secrecy." *Id.* With respect, the Court misread *Totten* and *Tenet*, neither of which turned on an "implicit" equitable estoppel theory. Rather, the Supreme Court explained explicitly in *Tenet* that *Totten's* rule "*was not so limited*," *see Tenet*, 544 U.S. at 9 (emphasis added), and that *any suit* that would inevitably lead to the disclosure of confidential information must be dismissed, *see id.* (emphasis added). Of course, disclosure of a classified relationship would cause the same harm to national security whether or not the plaintiff was a party to the alleged relationship. Because Plaintiffs' action here hinges on the existence of an asserted secret espionage relationship between MCI and/or Verizon and the NSA, *Totten* and *Tenet* are directly applicable.

(U) *Weinberger v. Catholic Action of Hawaii/Peace Educ. Project*, 454 U.S. 139 (1981)—cited by the Supreme Court in *Tenet*, 544 U.S. at 9—confirms the error in limiting *Tenet* and *Totten* to an "implicit" equitable estoppel theory. In *Weinberger*, the Supreme Court invoked *Totten* in dismissing a challenge under the National Environmental Protection Act ("NEPA"), where the determination of whether the Navy complied with NEPA was held to be beyond judicial scrutiny because, "due to national security reasons" the Navy could not admit or deny the central fact at issue in that suit as to whether it proposed to store nuclear weapons at a facility. *See* 454 U.S. at 147. Thus, the Supreme Court in *Weinberger* applied the *Totten* rule completely outside the context of an asserted espionage agreement, and precluded a lawsuit by someone with no alleged contractual relationship with the Government. *Weinberger* underscores that *Totten* is not a rule of "equitable estoppel."

(U) The Fourth Circuit's recent ruling in *El-Masri* is also instructive. There, as in this case, the plaintiff, who was not a party to an alleged espionage relationship, sued corporate and individual defendants, alleging their participation in secret and unlawful Government activity. The Fourth Circuit affirmed dismissal of the case on state secrets grounds, explaining that, for the litigation to proceed, plaintiff "would have to demonstrate the existence and details of [Government] espionage contracts, an endeavor practically indistinguishable from that categorically barred by *Totten* and *Tenet*." *El-Masri*, ___ F.3d at ___, 2007 WL 625130 at *9.

(U) Beyond this, the Court's conclusion in *Hepting* that "unlike the clandestine spy arrangements in *Tenet* and *Totten*, AT&T and the government have for all practical purposes already disclosed that AT&T assists the government in monitoring communication content," is also flawed for several reasons. *Hepting*, 439 F. Supp. 2d at 991. First, the Government's mere acknowledgment of a program (the TSP) not even challenged in *Hepting* (or here) surely cannot be read as an acknowledgment of any other program, nor can it be read as an acknowledgment of AT&T or Verizon's participation in any program. Nor does the simple fact of AT&T's size or publicly-stated willingness to assist generally with law enforcement matters provide any basis to conclude that AT&T assisted the NSA with any specific foreign intelligence program. *Totten* and *Tenet* are clear that the subject of a classified espionage relationship is *categorically barred* from litigation, and thus the very process undertaken by the Court of sifting through public statements to determine *whether* the case could proceed under *Totten* itself conflicted with that the rule established in that case.

(U) Furthermore, any public statements by the private party purportedly involved in the alleged relationship (AT&T in *Hepting* and Verizon here) are plainly irrelevant under *Totten* and *Tenet*. Indeed, unlike here, the plaintiffs in both of those cases would have *known* about their connection to the alleged espionage relationship. Nonetheless, the Supreme Court held that such relationships are not permissible topics of litigation. Where suits concerning alleged espionage relationships are categorically barred even where a party to that alleged relationship—an actual *witness* to the alleged matter—seeks to disclose its existence, it cannot be the case that parties with no actual knowledge can force disclosure of whether such a relationship existed. Under the Court's reasoning, if AT&T or Verizon sued the Government alleging that they had assisted in classified NSA activities and seeking to enforce a government contract with respect to such activities, the matter would have to be dismissed to protect national security, whereas a party with *no knowledge* of that alleged relationship could sue to force its very disclosure. That outcome is inconsistent with the purpose of the *Totten/Tenet* doctrine: to avoid disclosing information that public policy requires be maintained as confidential due to national security reasons, including impairing the nation's intelligence activities. *See Tenet*, 544 U.S. at 9.

2. (U) The State Secrets Privilege Also Requires Dismissal of this Action to Protect Whether or Not MCI/Verizon Assisted the NSA in the Alleged Activities.

(U) Even if the categorical bar to suit under the *Tenet/Totten* doctrine did not apply here, the state secrets privilege provides a distinct and independent ground for dismissing Plaintiffs' claims against the Verizon Defendants. The question presented by the state secrets privilege is whether facts confirming or denying Verizon's alleged assistance to the NSA with respect to the alleged activities are necessary to decide the case but would cause harm to national security if disclosed. If that is so, the case cannot proceed. Here, of course, it cannot be disputed that disclosure of whether or not Verizon assisted the NSA is essential to proceeding. Indeed, it is a key element of every one of Plaintiffs' claims. The Government has not confirmed or denied whether Verizon assisted with any of the alleged activities, and no grounds exist for finding that such information may be disclosed in this case in the face of the harms to national security identified by the DNI and NSA Director.

(U) *Alleged Content Surveillance Dragnet*: With respect to the surveillance of the content of communications, the Government's acknowledgment of the *existence* of the Terrorist Surveillance Program revealed nothing about whether particular telecommunication companies such as Verizon assisted with that program. The Court's analysis on this point in *Hepting*—that the NSA could not conduct the alleged activities without the assistance of the private sector—was based on the judicially noticed fact that AT&T is a large company. *See* 439 F. Supp. 2d at 991-92. But no public facts provide any basis to conclude that only large firms, and not small ones, would have the resources or expertise to furnish any needed assistance (if, indeed, there was any such assistance), or that the Government could not accomplish the alleged surveillance on its own. Similarly, the fact that AT&T has a history of providing some assistance to the Government, including on general law enforcement matters or some unspecified classified contracts, *see id.*, does not mean that the Government requested AT&T's assistance, or that AT&T provided assistance, with respect to the NSA surveillance activities alleged in *Hepting*. Indeed, even considering AT&T's general statements concerning its cooperation with the United States on unspecified projects, no relationship between AT&T and the NSA in connection with any of the activities alleged in *Hepting* has *ever* been confirmed or denied, and the public record provides no basis for inferring whether such a relationship exists. The Court was thus able to state only that "AT&T is assisting the government to implement *some kind* of surveillance program," and "AT&T and the government have *some kind* of intelligence relationship," *see id.* at 994 (emphasis added). Particularly where the Plaintiffs in *Hepting*, as here, are not even challenging the content surveillance program that was acknowledged by the President—the TSP—these conclusions were insufficient to override the judgment of the Director of National Intelligence on a matter of national security as to the harm that would result from confirming or denying an intelligence relationship with respect to specific allegations.

(U) The same is true in this case. Whether or not Verizon may have assisted the Government with classified or law enforcement matters in general says nothing about whether it has assisted the NSA in connection with the activities alleged in these cases. Similarly, the relative size of Verizon does not by itself indicate assistance as to a particular activity such as the TSP, especially where information about the operation of that activity has not been disclosed.

(U) The harms to national security at stake in confirming or denying an alleged intelligence relationship are indeed significant. Revealing whether or not Verizon assists the NSA with specific intelligence activities, for example, would replace speculation with certainty for hostile foreign adversaries who are balancing the risk that a particular channel of communication may not be secure against the need to communicate efficiently. Public McConnell Decl. ¶ 13. The Court itself recognized this concern with respect to the alleged communications records activities, when it observed in *Hepting* that "[a] terrorist who operates with full information is able to communicate more securely and more efficiently that a terrorist who operates in an atmosphere of uncertainty." *See id.* at 990. The DNI has set forth a more than reasonable basis to conclude that harm to national security would result from the disclosure of whether or not the NSA has worked with Verizon in connection with the alleged activities, and the Court has correctly observed that it is not in a position to second guess the DNI's judgment regarding a terrorist's risk preferences—a judgment which might depend on an array of facts not before the Court. *See Hepting,* 439 F. Supp. 2d at 990, 997.

(U) Weighed against these considerations is the mere allegation, based on conjecture and media reports, that Verizon must be assisting the NSA with certain alleged intelligence activities without judicial supervision. *See, e.g.,* Master Verizon Complaint ¶¶142-62. Such unconfirmed speculation cannot outweigh the DNI's assertion of privilege and the harms he has identified. The Court has already rejected reliance on information in media reports to undercut a state secrets privilege assertion. *See Hepting*, 439 F. Supp. 2d at 989-90. Indeed, reliance on such reports would improperly place national security decisions in the hands of reporters whose sources often speculate as to government activity and whose reporting in any event will not always be presumed accurate or reliable by the public. It would also require the United States to officially confirm or deny such reporting when the government has not previously done so. That outcome would largely eviscerate the state secrets privilege and is contrary to cases that affirm the Government's right to protect national security information if the Government has not officially disclosed the precise information to the public. Even when alleged facts have been the "subject of widespread media and public speculation" based on "[u]nofficial leaks and public surmise," those alleged facts are not actually established in the public domain. *Afshar v. Department of State,* 702 F.2d 1125, 1130-31 (D.C. Cir. 1983); *see also Fitzgerald,* 776 F.2d at 1242-43 (affirming dismissal because subject was state secret despite published article on the matter); *Edmonds v. FBI*, 272 F. Supp. 2d at 49 (because statements in the press were made by anonymous sources, even documents containing identical information may properly be withheld because "release would amount to official confirmation or acknowledgment of their accuracy").

(U) In a case directly on point, the Court in *Terkel* expressly held that the Government had not confirmed or denied involvement by AT&T in the alleged communication records program and that it would "undermine the important public policy underlying the state secrets privilege if the government's hand could be forced by unconfirmed allegations in the press or by anonymous leakers whose disclosures have not been confirmed." *Terkel v. AT&T*, 441 F. Supp. 2d at 913-14 (holding that media reports of alleged NSA programs "amount to nothing more than unconfirmed speculation").

(U) Similarly, public statements by Verizon itself, *see* Master Verizon Compl. ¶¶ 160-61, are irrelevant to the state secrets privilege inquiry. As the Supreme Court has admonished, the state secrets privilege "belongs to the Government" and cannot be "waived by a private party." *Reynolds*, 345 U.S. at 7; *see Kasza*, 133 F.3d at 1165. Thus, in inquiring whether a relationship had been confirmed or denied, the Court in *Hepting* should have limited itself to authoritative Government statements and should not have looked to statements by other persons or entities. As the courts have recognized, "disclosure of information by government officials can be prejudicial to government interests, even if the information has already been divulged from non-government sources." *Bareford v. General Dynamics Corp.*, 973 F.2d at 1144 (5th Cir. 1992).[16]

(U) *Alleged Communication Records Collection*: With respect to the alleged collection of communication records information, the Court in *Hepting* agreed that the authorized Executive Branch officials have not confirmed this activity, let alone a telecommunication carrier's assistance in the matter. *See Hepting*, 4430 F. Supp. 2d at 997. And although the Court erred in our view by declining to dismiss this claim in *Hepting* because of the possibility that the Government or telecommunication carriers "might disclose, either deliberately or accidentally, other pertinent information about the communication records program as this litigation proceeds," and that "such disclosures might make this program's existence or non-existence no longer a secret," *id.* at 997-98, nothing warrants proceeding with these allegations in this case. As the Court noted:

> Revealing that a communications records program exists might encourage that terrorist to switch to less efficient but less detectable forms of communication. And revealing that such a program does not exist might encourage a terrorist to use [a provider's] services when he would not have done so otherwise.

Hepting, 439 F. Supp. 2d at 997; *accord Terkel v. AT&T*, 441 F. Supp. 2d at 915 (requiring telecommunications carrier to admit or deny existence of Government request to assist on alleged communications records program would disclose significant information that had not been revealed by other public information). Even a small margin of error may make the difference in protecting national security. Under these circumstances, and in light of the highly deferential standard of review under the state secrets privilege, for the Court to conclude based on limited public facts that the Executive Branch must confirm or deny alleged intelligence sources or methods, where such disclosures may pose grave or even unforeseeable consequences, would be misguided and inappropriate.

---

[16] **(U)** Any effort to use this litigation to ascertain the meaning of Verizon's statements would plainly require discovery and confirmation of whether and to what extent MCI or Verizon assisted the Government and whether and to what extent the alleged activities even existed—that is, it would require *new and additional* facts that are subject to the state secrets privilege assertion.

[REDACTED TEXT]

* * *

(U) Because confirming or denying the alleged relationship between the NSA and the Verizon Defendants could reasonably be expected to cause the harms to national security described by the DNI and NSA Director, and because adjudicating Plaintiffs' claims will necessarily require confirming or denying such a relationship, the case must be dismissed. Dismissal is required regardless of whether the matter is considered to be the "very subject matter" of the case, or because facts concerning the alleged relationship would be needed for Plaintiffs' to make a *prima facie* case or for a defense to be presented. The issue remains the same: facts concerning Verizon's alleged relationship with the NSA must be placed into evidence for this case to proceed, and doing so would plainly harm the national security interests of the United States.

B. (U) Whether or Not Plaintiffs Have Standing Cannot be Established or Refuted Without the Disclosure of State Secrets and Harm to National Security.

(U) Aside from whether MCI or Verizon had any involvement in the alleged NSA activities, the equally fundamental issue of Plaintiffs' standing cannot be adjudicated without state secrets. As is well known, the Constitution "limits the jurisdiction of federal courts to 'Cases' and 'Controversies,'" and "the core component of standing is an essential and unchanging part of th[is] case-or-controversy requirement." *Lujan v. Defenders of Wildlife*, 504

U.S. 555, 559-60 (1992). Plaintiffs, of course, bear the burden of establishing standing and must, at an "irreducible constitutional minimum," demonstrate (1) an injury-in-fact, (2) a causal connection between the injury and the conduct complained of, and (3) a likelihood that the injury will be redressed by a favorable decision. *Id.* In meeting that burden, the named Plaintiffs must demonstrate an actual or imminent—not speculative or hypothetical—injury that is particularized as to them; they cannot rely on alleged injuries to unnamed members of a purported class.[17] Moreover, to obtain prospective relief, Plaintiffs must show that they are "immediately in danger of sustaining some direct injury" as the result of the challenged conduct. *City of Los Angeles v. Lyons,* 461 U.S. 95, 102 (1983); *O'Shea v. Littleton,* 414 U.S. 488, 495-96 (1974).[18]

(U) A plaintiff must demonstrate Article III standing for "each claim he seeks to press," *DaimlerChrysler Corp. v. Cuno*, 126 S. Ct. 1854, 1867 (2006), and must further establish "prudential" standing by showing that "the constitutional or statutory provision on which [each] claim rests properly can be understood as granting persons in the plaintiff's position a right to judicial relief." *Warth*, 422 U.S. at 499-500. To do so, a plaintiff normally "'must assert his own legal rights and interests, and cannot rest his claim to relief on the legal rights or interests of third parties.'" *Smelt v. County of Orange*, 447 F.3d 673, 682 (9th Cir. 2006) (quoting *Phillips Petroleum Co. v. Shutts*, 472 U.S. 797, 804 (1985)). To advance a statutory claim, a plaintiff must show that his particular injury "fall[s] within 'the zone of interests to be protected or regulated by the statute'" in question. *Id.* at 683.

---

[17] **(U)** *See, e.g., Warth v. Seldin*, 422 U.S. 490, 502 (1975) (the named plaintiffs in an action "must allege and show that they personally have been injured, not that injury has been suffered by other, unidentified members of the class to which they belong and which they purport to represent").

[18] **(U)** Standing requirements demand the "strictest adherence" when, like here, constitutional questions are presented and "matters of great national significance are at stake." *Elk Grove Unified Sch. Dist. v. Newdow,* 542 U.S. 1, 11 (2004); *see also Raines v. Byrd,* 521 U.S. 811, 819-20 (1997) ("[O]ur standing inquiry has been especially rigorous when reaching the merits of the dispute would force us to decide whether an action taken by one of the other two branches of the Federal Government was unconstitutional."); *Schlesinger v. Reservists Comm. to Stop the War*, 418 U.S. 208, 221 (1974) ("[W]hen a court is asked to undertake constitutional adjudication, the most important and delicate of its responsibilities, the requirement of concrete injury further serves the function of insuring that such adjudication does not take place unnecessarily.").

(U) Here, the state secrets privilege prevents Plaintiffs from establishing, and Defendants from refuting, any injury because it bars proof of whether Plaintiffs have been subject to the alleged surveillance activities.[19] As discussed, the Government's privilege assertion covers, *inter alia*, any information (1) tending to confirm or deny whether the Plaintiffs were subject to any of the alleged intelligence activities at issue, (2) tending to confirm or deny whether Verizon is involved with particular alleged intelligence activities, and (3) concerning the alleged activities, including program facts demonstrating that the TSP was limited to one-end foreign al Qaeda communications and was not the dragnet that Plaintiffs allege, and facts that would confirm or deny the existence of the alleged communications records activities. *See* Public McConnell Decl. ¶ 16. Without these facts—the disclosure of which would harm national security for reasons explained by the DNI and NSA Director—Plaintiffs cannot establish any alleged injury that is fairly traceable to Verizon.

(U) It is important to emphasize the procedural posture of the Government's pending motions as they pertain to this standing issue. Whether the Plaintiffs can establish their standing is not merely a question to be decided on the pleadings. Regardless of whether Plaintiffs adequately allege injury to get past the pleading stage, the United States, through its motion for summary judgment, has specifically put at issue whether the named Plaintiffs will be able to sustain their burden of *proving* a concrete, personal injury *as a factual matter* in light of the state secrets privilege assertion.[20] Given the Government's summary judgment motion, the Plaintiffs cannot rest on general allegations in their complaints, but must be able to set forth specific facts by affidavit or evidence that would support their standing to obtain the relief sought. *See Lewis v. Casey*, 518 U.S. 343, 358 (1996) (quoting *Lujan*, 504 U.S. at 561). The issue raised by the Government's motion is whether that will be possible where the DNI has properly asserted privilege over facts tending to confirm or deny the application of alleged intelligence activities to particular individuals, including the named Plaintiffs in this case. Because the DNI has set forth reasonable grounds to protect such information, the facts needed to establish or refute the Plaintiffs' standing cannot be disclosed and the case thus cannot proceed. This is not an issue that can be deferred. If Plaintiffs' claims of injury cannot be proven without disclosing state secrets and harming national security—and we submit they cannot—then judgment must be entered in favor of the Defendants now.

---

[19] **(U)** The focus herein is on Plaintiffs' inability to prove standing because it is their burden to demonstrate jurisdiction. *See Lujan*, 504 U.S. at 561. Dismissal of this action, however, is also required for the equally important reason that the MCI and Verizon Defendants and the United States as intervenor would not be able to present any evidence disproving standing on any claim without revealing information covered by the state secrets privilege assertion (*e.g.*, whether or not a particular person's communications were intercepted). *See Halkin I*, 598 F.2d at 11 (rejecting plaintiffs' argument that the acquisition of a plaintiff's communications may be presumed from the existence of a name on a watchlist, because "such a presumption would be unfair to the individual defendants who would have no way to rebut it").

(U) In *Hepting*, the United States argued, as it has here, that the plaintiffs would be unable to establish standing absent state secrets. In addressing that issue, the Court referred to its prior conclusion that "the state secrets privilege will not prevent plaintiffs from receiving at least some evidence tending to establish the factual predicate of the injury-in-fact underlying their claims directed at AT&T's alleged involvement in the monitoring of communication content." 439 F. Supp. 2d at 1001. With respect, the Court's conclusion in *Hepting* as to the impact of the state secrets privilege on the plaintiffs' standing was in error. By focusing solely on the issue of AT&T's alleged involvement, the Court disregarded the critical factual issue related to standing: whether the *individual plaintiffs* had in fact been subjected to the alleged intelligence activities. That issue exists apart from whether AT&T had any involvement in the alleged activities, because if the plaintiffs were not injured, they could not establish their standing regardless of whether AT&T assisted the NSA with content surveillance.

---

[20] **(U)** The Court can dismiss this case on the pleadings under the *Totten/Tenet* rule and the "very subject matter" prong of the state secrets privilege. The Government's summary judgment motion is made in the alternative because, if the Court declines to dismiss on those grounds, the questions of whether the state secrets privilege precludes Plaintiffs from proving their standing or making a *prima facie* case, or Defendants from presenting a defense, are more properly considered as summary judgment questions. *See Zuckerbraun*, 935 F.2d at 547. Indeed, the Government's summary judgment motion places the burden on Plaintiffs to prove their standing and to make out a *prima facie* case without state secrets, which they cannot do.

1. (U) Plaintiffs Cannot Establish Standing Because The State Secrets Privilege Forecloses Litigation Over Whether They Have Been Subject To Surveillance.

(U) The issue of whether Plaintiffs can file a lawsuit alleging unlawful foreign intelligence surveillance and then seek, in the first instance, to discover whether they have actually been subject to such surveillance is not a new one. Courts have consistently refused to recognize standing to challenge a Government surveillance program where the state secrets privilege prevents a plaintiff from establishing, and the Government from refuting, that he was actually subject to surveillance.

(U) In *Halkin I*, for example, a number of individuals and organizations claimed that they were subject to unlawful surveillance by the NSA and CIA (among other agencies) due to their opposition to the Vietnam War. *See* 598 F.2d at 3. The D.C. Circuit upheld an assertion of the state secrets privilege regarding the identities of individuals subject to NSA surveillance, rejecting the plaintiffs' argument that the privilege could not extend to the "mere fact of interception," *id.* at 8, and despite significant public disclosures about the surveillance activities at issue, *id.* at 10.[21]

(U) A similar state secrets assertion with respect to the identities of individuals subject to CIA surveillance was upheld in *Halkin II.* See 690 F.2d at 991. There, as here, the plaintiffs claimed that alleged NSA surveillance of their communications violated the Fourth Amendment. Plaintiffs relied on the claim that their names were included on "watchlists" used to govern NSA surveillance, arguing that this fact demonstrated a "substantial threat" that their communications would be intercepted. *See id.* at 983-84, 997. The D.C. Circuit nevertheless affirmed dismissal of the Fourth Amendment claim, "hold[ing] that appellants' inability to adduce proof of actual acquisition of their communications" rendered them "incapable of making the showing necessary to establish their standing to seek relief." *Id.* at 998. As here, plaintiffs "alleged, but ultimately cannot show, a concrete injury" in light of the Government's invocation of the state secrets privilege. *Id.* at 999.[22] The court thus found dismissal warranted, even though the complaint alleged actual interception of plaintiffs' communications, because the plaintiffs' alleged injuries could be no more than speculative in the absence of their ability to prove that such interception occurred.[23] *Id.* at 999, 1001; *see also Ellsberg*, 709 F.2d 51 (also holding that dismissal was warranted where a plaintiff could not, absent recourse to state secrets, establish that he was actually subject to surveillance).

---

[21] **(U)** As the court of appeals recognized, the "identification of the individuals or organizations whose communications have or have not been acquired presents a reasonable danger that state secrets would be revealed . . . [and] can be useful information to a sophisticated intelligence analyst." *Halkin I*, 598 F.2d at 9.

[22] **(U)** See *Halkin II*, 690 F.2d at 990 ("Without access to the facts about the identities of particular plaintiffs who were subjected to CIA surveillance (or to NSA interception at the instance of the CIA), direct injury in fact to any of the plaintiffs would not have been susceptible of proof."); *id.* at 987 ("Without access to documents identifying either the subjects of . . . surveillance or the types of surveillance used against particular plaintiffs, the likelihood of establishing injury in fact, causation by the defendants, violations of substantive constitutional provisions, or the quantum of damages was clearly minimal.").

[23] **(U)** Because the CIA conceded that nine plaintiffs were subjected to certain types of non-NSA surveillance, the D.C. Circuit held that those plaintiffs had demonstrated an

(U) In addition to foreclosing Plaintiffs' ability to prove standing for their constitutional claims as in *Halkin*, the state secrets privilege would preclude Plaintiffs from establishing standing as to their statutory claims. For example, FISA authorizes only an "aggrieved person" to bring a civil action challenging the acquisition of communications contents. 50 U.S.C. §§ 1801(f), 1810. To ensure that this term would be "coextensive [with], but no broader than, those persons who have standing to raise claims under the Fourth Amendment with respect to electronic surveillance," H.R. Rep. No. 95-1283, at 66 (1978), Congress defined "aggrieved person" to mean one "whose communications or activities were *subject to* electronic surveillance," 50 U.S.C. § 1801(k) (emphasis added). Litigants who cannot establish their status as "aggrieved persons" therefore do "not have standing" under "any" of FISA's provisions. H.R. Rep. No. 95-1283, at 89-90; cf. *United States v. Ott*, 827 F.2d 473, 475 n.1 (9th Cir. 1987); *see also Director, Office of Workers' Comp. Programs v. Newport News Shipbuilding & Dry Dock Co.*, 514 U.S. 122, 126 (1995) ("aggrieved" is a well-known term of art used "to designate those who have standing").

(U) Title III similarly specifies that civil actions may be brought by a "person whose . . . communication *is* intercepted, disclosed, or intentionally used." 18 U.S.C. § 2520(a) (emphasis added). The Stored Communications Act likewise limits its civil remedies to "person[s] aggrieved" under that statute, see 18 U.S.C. § 2707(a), and the only persons aggrieved by a communication-service provider's "knowing[] divulge[nce]" of the "contents of a

---

injury-in-fact. *See Halkin II*, 690 F.2d at 1003. Nonetheless, the nine plaintiffs were precluded from seeking injunctive and declaratory relief because they could not demonstrate the likelihood of future injury or a live controversy in light of the fact that the CIA had terminated the specific intelligence methods at issue. *See id.* at 1005–09.

communication" or of customer records, 18 U.S.C. § 2702(a), are those persons whose communications or records were actually divulged. See 18 U.S.C. § 2711(1) (adopting § 2510(11) definition of "aggrieved person" as one "who was a party to any intercepted . . . communication" or "a person against whom the interception was directed"). Plaintiffs additionally seek relief under 47 U.S.C. § 605, but this statute makes equally clear that only a "person aggrieved" may challenge allegedly unlawful "divulge[nce] or publi[cation]" of the contents of a communication, see 47 U.S.C. §§ 605(a), (e)(3)(A), and "only a party to a tapped conversation may complain" of an alleged disclosure under § 605. See *United States ex rel. Ross v. LaVallee*, 341 F.2d 823, 824 (2d Cir. 1965). Each of these provisions reflects the fundamental point that only persons whose rights were injured by the actual interception or disclosure of their own communications (or records) have standing. Put simply, to recover damages, a plaintiff has to show that his or her rights were injured—and that cannot be done here.

(U) With respect, we disagree with the Court's statement in *Hepting* that allowing further proceedings, such as discovery, before assessing the full impact of the state secrets privilege would be consistent with *Halkin* and *Ellsberg*. *See Hepting*, 439 F. Supp. 2d at 994. In *Halkin I*, the Government immediately moved to dismiss on state secrets grounds to protect facts such as those at issue here—whether the plaintiffs were subject to surveillance and the methods and techniques by which communications were intercepted. *See* 598 F.2d at 4-5. The Government also opposed discovery requests, and responded only to court-propounded inquires with a state secrets privilege assertion. *See id.* at 6. The district court upheld the claim of privilege and dismissed the case as to one surveillance program (called MINARET), but denied dismissal as to a separate program (called SHAMROCK) as to which some information had been made public in Congressional hearings. *See id.* at 5. The Court of Appeals upheld the privilege assertion and dismissal as to the MINARET program and *reversed* the district court and upheld the privilege assertion as to the SHAMROCK program. *See* 598 F.2d at 8-11. Specifically with respect to discovery, the Court of Appeals said:

> In the case before us the acquisition of plaintiffs' communications is a fact vital to their claim. No amount of ingenuity of counsel in putting questions on discovery can outflank the government's objection that disclosure of this fact is protected by privilege. Thus, in these special circumstances, we conclude that affording additional discovery for the government to parry plaintiffs' requests would be fruitless. *In camera* resolution of the state secrets question was inevitable.

Halkin I, 598 F.2d at 6-7. As a result of this ruling, the claims against the NSA challenging the alleged surveillance of the plaintiffs were dismissed on remand without any discovery. *See Halkin II*, 690 F.2d at 984.

(U) A separate claim proceeded against the CIA for allegedly providing "watchlisting" information to the NSA that was used to undertake surveillance. *See Halkin II*, 690 F.2d at 984. While some document discovery occurred as to the defunct surveillance program at issue, which had been the subject of a Congressional investigation, the CIA nonetheless successfully asserted the state secrets privilege as to several facts, including whether any of the plaintiffs' names had been submitted on any watchlists to the NSA. *See id.* at 985. The district court concluded that, since the very fact of any interception was protected by NSA's state secrets assertion, the plaintiffs would be unable to prove any liability on the part of CIA, and thus dismissed those claims. The Court of Appeals affirmed, again upholding the state secrets privilege to bar disclosure of the identities of individuals subject to surveillance, *see id.* at 988-89, 993 n.57, and affirming dismissal for lack of standing, *see id.* at 997-1000. *See also id.* at 998 ("Since it is the constitutionality of such interceptions that is the ultimate issue, the impossibility of proving that interception of any [plaintiffs'] communications ever occurred renders the inquiry pointless from the outset."). Thus, *Halkin II* likewise supports dismissal of claims challenging alleged surveillance on state secrets grounds and without discovery. Whatever discovery that did occur in *Halkin* was therefore irrelevant and wasteful, because the threshold fact of whether the plaintiffs had been subject to surveillance could not be disclosed. Similarly, with respect to those plaintiffs whom the government in *Ellsberg* had not admitted overhearing, the court found that they lack an essential element of their proof of standing and that dismissal of their claims was therefore proper. *See* 709 F.2d at 65.

(U) The same result is required here. Because the state secrets privilege precludes the named Plaintiffs from demonstrating that they personally have been subject to surveillance activities, litigation over Plaintiffs' standing is foreclosed. As explained in non-classified terms by the DNI and NSA Director, the United States cannot confirm or deny whether any individual is subject to alleged surveillance activities without causing potentially grave harm to the national security, including by tending to reveal actual targets, sources, or methods. *See* Public McConnell Decl. ¶ 14; Public Alexander Decl. ¶ 15. For example, if the NSA were to confirm in this case and others that specific individuals are not targets of surveillance, but later refuse to comment (as it would have to) in a case involving an actual target, a person could easily deduce by comparing such responses that the person in the latter case is a target.

(U) The harm of revealing targets of foreign intelligence surveillance is obvious. If an individual knows or suspects he is a target of U.S. intelligence activities, he would naturally tend to alter his behavior to take new precautions against surveillance. *See id*; *see also Halkin I*, 598 F.2d at 9 ("the identity of particular individuals whose communications have been acquired can be useful information to a sophisticated intelligence analyst"). Revealing who is not a target, in turn, would indicate who has avoided surveillance and who may be a secure channel for communication. *See* Public McConnell Decl. ¶ 14; Public Alexander Decl. ¶ 15. Such information could lead a person, secure in the knowledge that he is not under surveillance, to help a hostile foreign adversary convey information; alternatively, such a person may be unwittingly utilized or even forced to convey information through a secure channel. *See id.* Revealing which channels are free from surveillance and which are not would also reveal sensitive intelligence methods and thereby could help any adversary evade detection. *See id.* The consequences of identifying who is and is not subject to alleged surveillance activities may vary depending on the circumstances. It is important to realize, however, that even a small piece of information related to one individual Plaintiff could represent, to a sophisticated adversary, an important "piece of the puzzle" of U.S. intelligence operations. *See Halkin I*, 598 F.2d at 8-9 ("[t]he significance of one item of information may frequently depend upon knowledge of many other items of information" and "what may seem trivial to the uninformed, may appear of great moment to one who has a broad view of the scene and may put the questioned item of information in its proper context.").

2. (U) Plaintiffs Cannot Establish Standing On The Basis Of A "Dragnet" Theory of Surveillance.

(U) It bears specifically noting that Plaintiffs' allegation of a "dragnet" of surveillance by the Verizon Defendants—the interception of millions of domestic and international communications made by ordinary Americans and transmitted by MCI and Verizon, *see, e.g., id.* ¶¶ 3, 165—does not establish their standing. Even if that allegation were sufficient to avoid dismissal through a standard Rule 12(b)(1) motion, facts concerning whether Plaintiffs have been subject to any such dragnet of surveillance would obviously be essential to adjudicate their standing for purposes of summary judgment.

(U) As an initial matter, the Plaintiffs have not even *alleged* that their communications have been intercepted under the Terrorist Surveillance Program acknowledged by the President. Indeed, the various complaints against the Verizon and MCI Defendants avoid any suggestion that Plaintiffs might fall within the acknowledged and limited scope of the TSP.[24] Moreover, the Court has already recognized that, in acknowledging that the TSP was a limited program aimed at tracking international communications of members or agents of al Qaeda and affiliated terrorist organizations, the Government denied that it was conducting the type of domestic content dragnet that Plaintiffs allege. *See Hepting*, 439 F. Supp. 2d at 996. In order to prove their standing for purposes of surviving the Government's summary judgment motion, therefore, the named Plaintiffs are required to come forward with specific evidence rebutting the Government's denial and establishing that they personally were subject to content surveillance. But that cannot be done in light of the state secrets assertion. As previously explained, the DNI has asserted the state secrets privilege over any information tending to confirm or deny whether Plaintiffs were subject to surveillance, as well as program information about the TSP that Plaintiffs likely would want disclosed to test, as an evidentiary matter, the limited scope of that program. Because none of that information can be disclosed without revealing intelligence targets, sources, and methods, Plaintiffs are not able to confirm or deny that they personally were subject to surveillance (either under the TSP or their alleged domestic dragnet). Similarly, in light of the privilege, Defendants are not able to offer evidence that would demonstrate any lack of standing. Accordingly, summary judgment must be granted against the Plaintiffs.

---

[24] **(U)** Accordingly, even if Plaintiffs did purport to challenge the TSP, they would lack standing to do so on the face of their complaint.

[REDACTED TEXT]

3. (U) Plaintiffs' Standing to Challenge Alleged Collection of Communication Records Information Cannot be Adjudicated Without State Secrets.

(U) Plaintiffs' standing to challenge the alleged assistance of the Verizon Defendants with an alleged program by the NSA to collect records about their communications, *see* Master Verizon Compl. ¶ 226, cannot be adjudicated for the same reasons. The facts needed to adjudicate standing would include not only *whether* such a program existed but, even if it did exist and could be acknowledged by the Government, whether and how it may impact the

Plaintiffs. Disclosure of such information would again reveal intelligence sources and methods, confirming for our adversaries the nature and scope of what the Government does or does not do and thereby enabling them to avoid detection.

[REDACTED TEXT]

C. (U) The Disclosure of Facts Concerning the Alleged NSA Intelligence Activities Is Required to Adjudicate Plaintiffs' Claims on the Merits.

(U) As with the threshold issues of relationship and standing, Plaintiffs cannot prove the merits of their case without establishing the existence of the alleged activities, that the Verizon Defendants were involved in such activities, and that they are personally subject to such activities—all of which is precluded by the state secrets privilege. And even assuming *arguendo* that these threshold facts could be established (a possibility the Government disputes), the merits of Plaintiffs' claims also could not be adjudicated without facts about the operation of any alleged activity, including the precise nature of the activities, how they were conducted, why they were conducted, when they were conducted and for how long, and the intelligence value of the activities.

1. (U) Plaintiffs' Claims as to Alleged Warrantless Content Surveillance Cannot be Adjudicated Without Disclosing State Secrets.

(U) This lawsuit commenced after media reports in December 2005 alleged that the NSA was engaged in certain surveillance activities. *See* Master Verizon Compl. ¶¶ 138, 142; *Chulsky* Compl. ¶¶ 18, 24; *Riordan* Compl. ¶ 20; *see also Hepting*, 439 F. Supp. 2d at 986. Plaintiffs cite statements made at the time by the President, the Attorney General, and the Deputy Director of National Intelligence acknowledging that the President had authorized the NSA to intercept the content of one-end foreign communications where a party to the communication was reasonably believed to be a member or agent of al Qaeda or an affiliated terrorist organization. For example, the President has stated that the TSP was limited to surveillance of communications and individuals associated with al Qaeda and did not involve the interception of purely domestic calls in the United States. *See Hepting*, 439 F. Supp. 2d at 987 (taking judicial notice of President's statement that the government's "international activities strictly target al Qaeda and their know affiliates" and that "the government does not listen to domestic phone calls without approval" and that the government is "not mining or trolling through the personal lives of millions of Americans."); *see also* Master Verizon Compl. ¶ 139; *Chulsky* Compl. ¶ 25 (citing statement by President on TSP). Attorney General Gonzales has likewise stated that the TSP does not involve the interception of domestic to domestic calls within the United States. *See Hepting*, 439 F. Supp. 2d at 987 (citing statements); *see also* Verizon Master Compl. ¶ 141; *Chulsky* Compl. ¶ 26. Then-Deputy DNI, Gen. Michael Hayden, also stated regarding the scope of the TSP:

> The purpose of all this is not to collect reams of intelligence, but to detect and prevent attacks. The intelligence community has neither the time, the resources, nor the legal authority to read communications that aren't likely to protect us, and the NSA has no interest in doing so. These are communications that we have reason to believe are al Qaeda communications, a judgment made by intelligence professionals. . . . This is targeted and focused. This is not about intercepting conversations between people in the United States. This is hot pursuit of communications entering or leaving America involving someone we believe is associated with al Qaeda.

See Remarks of Gen. Michael V. Hayden, National Press Club, Jan. 23, 2006.

(U) Despite these plain denials that the TSP was a domestic content dragnet—denials which the Court in *Hepting* acknowledged, *see* 439 F. Supp. 2d at 996—Plaintiffs allege without any foundation, based on a newspaper article, that "the NSA intercepts *millions* of communications made or received by people inside the United States" as part of a "massive surveillance operation" for "data-mining" the "content" of millions of communications to find those of particular interest. *See* Verizon Master Compl. ¶¶ 165, 167. They claim that the NSA intercepts "*all* or a substantial number of the communications transmitted through [Verizon's] key domestic telecommunication facilities, including direct access to streams of domestic, international, and foreign telephone and electronic communications." *Id.* ¶ 168. *See Hepting*, 439 F. Supp. 2d at 994 ("Plaintiffs allege a surveillance program of far greater scope than the publicly disclosed 'terrorist surveillance program.'"). In short, through their content surveillance claim, Plaintiffs seek to prove whether the Government's statements about the limited nature of the TSP are true or whether Plaintiffs' alleged dragnet actually exists and covered their own communications. Plaintiffs thus allege that the NSA undertakes a secret content surveillance program *other than and broader than* the TSP.

(U) The Court's conclusion in *Hepting* that the Government's acknowledgment of the existence of the TSP has "opened the door for judicial inquiry" into the scope of any content monitoring program undertaken by the NSA, *Hepting*, 433 F. Supp. 2d at 996, is unfounded in our view (and is among the issues now on appeal). If such a disclosure did open the door to further inquiry, state secrets would be needed to walk through it. The Court in *Hepting* recognized that the Government "has disclosed the universe of possibilities in terms of *whose* communications its monitors and *where* those communicating parties are located." *See id.* As the President stated, that universe involved the surveillance of communications (1) made by parties reasonably believed to be members or agents of al Qaeda or affiliated terrorist organizations, and (2) sent to or from the United States. But proving or disproving those two facts as an evidentiary matter, in order to adjudicate Plaintiffs' dragnet allegation, would require the disclosure of TSP program information and perhaps other NSA surveillance methods and activities, to show that the alleged dragnet of millions of domestic communications is not occurring.[25] As set forth in the privilege assertions of DNI McConnell and NSA Director

---

[25] **(U)** To the extent the Court in *Hepting* suggested that the proof needed to address whether or not the alleged domestic content surveillance dragnet exists might be found in the scope of any certification to a telecommunications carrier, *see id.* at 996-97, we again respectfully disagree. That very relationship issue is among the matters subject to the Government's privilege

Alexander, those facts cannot be disclosed without causing exceptionally grave harm to national security.

[REDACTED TEXT]

(U) The foregoing demonstrates that the TSP authorized by the President after 9/11 was not directed at generalized domestic surveillance of the content of communications of millions of Americans, as Plaintiffs allege. Moreover, to demonstrate that no *other* NSA program involves the alleged domestic content dragnet, proof beyond the operation of the TSP would have to be offered to demonstrate these facts (again, by having to prove a negative). But such information also could not be disclosed without revealing sensitive NSA sources and methods to our adversaries and thereby causing harm to the national security. Courts cannot allow litigants "to force 'groundless fishing expeditions' upon them," *Sterling*, 416 F.3d at 344, and a plaintiff is not permitted to "embark on a fishing expedition in government waters on the basis of [its own] speculation," *Ellsberg v. Mitchell*, 807 F.2d 204, 207-08 (D.C. Cir. 1986) (Scalia, Circuit Justice) ("*Ellsberg II*"). Litigation cannot proceed on claims where discovery of the actual facts needed to prove or rebut allegations is barred by the state secrets privilege. *See Molerio v. Federal Bureau of Investigation*, 749 F. 2d 815, 826 (D.C. Cir. 1984) (it would be "a mockery of justice" to permit further proceedings where the actual facts are privileged).[26]

---

assertion, and to put that matter at risk in order to demonstrate that an allegation *already denied by the Government* is false, would be unfounded.

[26] **(U)** Because Plaintiffs neither allege that the TSP applies to them nor challenge that program, the lawfulness of the TSP is not at issue here. Even if they did challenge the TSP, however, classified details about the program, as described in the *In Camera* Alexander Declaration, would be needed to adjudicate its lawfulness.

2. (U) Plaintiffs' Challenge to Alleged Communication Records Collection Cannot be Adjudicated Without Disclosing State Secrets.

(U) Plaintiffs' challenge to the alleged collection of communication records likewise cannot be adjudicated without disclosing state secrets. *See Terkel*, 441 F. Supp. 2d at 919-20 (holding that disclosure of whether or not AT&T has assisted the government's intelligence activities by providing large quantities of telephone records "would adversely affect our national security" and therefore is "barred by the state secrets privilege"). The Court in *Hepting* correctly found that information confirming or denying an alleged communication records program should remain protected from disclosure. *See* 439 F. Supp. 2d at 997-98. Indeed, the Court recognized the potential harm of confirming or denying such allegations, and it also appropriately held that it is not in a position to second-guess the judgment of the DNI and NSA Director regarding such harm.

(U) At the same time, we respectfully believe that the Court's decision not to dismiss the records claim—a decision based on the "conceivable" possibility that deliberate or even accidental disclosures about the records allegations could be made in the future—was erroneous. *See id.* at 997. First, the Government has consistently maintained that the records allegations could not be confirmed or denied without harming national security, and it is inappropriate for the Court to keep the claims open on the chance that such harmful disclosures might be made, even accidentally, at some undetermined future date. Moreover, the suggestion that public disclosures of private entities might waive the state secrets privilege is incorrect. As outlined above, whether information may be protected under the state secrets privilege turns on whether the Government has reasonably shown that harm would flow from disclosure of that information. Unless an authorized official of the United States Government formally confirms or denies the existence of an alleged activity, any other public statement or disclosure, particularly "accidental" ones, cannot trump the Government's assertion of privilege. For these reasons, the Court in *Terkel* correctly dismissed a case alleging that AT&T participated in an illegal record program. *See* 441 F. Supp. 2d at 916, 919-20. To the extent this Court has any remaining doubts about whether the records claims should be dismissed here, we wish to emphasize the following.

[REDACTED TEXT]

(U) Assuming, *arguendo*, that the alleged records program did exist and was confirmed by the Government, numerous facts about the operation of any such program would be needed to determine its lawfulness, including how the activity proceeds, whose information may be collected, what may be done with the information, and why the information may be collected—all of which, if such activity occurred, would reveal intelligence sources and methods to our adversaries. For example, civil liability provisions of the Stored Communications Act require proof of actual damages by the plaintiff, *see* 18 U.S.C. § 2707(c), and that would require showing that an action was taken against an individual plaintiff that caused that person actual damages. Similarly, the Supreme Court has held that an individual has no Fourth Amendment protected legitimate expectation of privacy regarding the numbers dialed on a telephone, *see Smith v. Maryland*, 442 U.S. 735, 742 (1979), and this issue could not be adjudicated without describing the extent to which the NSA, if it does at all, collects data in which there is an expectation of privacy. Similarly, the need for any such activity would be relevant evidence in deciding the lawfulness of such a program, *see Vernonia Sch. Dist. v. Action*, 515 U.S. 646, 653 (1995) (there are circumstances when special needs, beyond the normal need for law enforcement, make the warrant and probable cause requirement impracticable).[27] Finally, the efficacy of a challenged activity is another factor in assessing it lawfulness. *See Vernonia*, 515 U.S. at 663. Thus, even assuming purely for the sake of argument that one could show that a particular activity is occurring, the evidence needed to adjudicate a challenge on the merits implicates host of different facts, all of which implicate the existence, scope, and nature of alleged intelligence sources and methods.

---

[27] **(U)** Similarly, the Stored Communications Act provides that a telecommunication carrier may divulge customer records "to a governmental entity, if the provider reasonably believes that an emergency involving immediate danger or death or serious physical injury to any person justifies disclosure of the information." 18 U.S.C. § 2702(c)(4).

[REDACTED TEXT]

IV. (U) STATUTORY PRIVILEGE CLAIMS HAVE ALSO BEEN PROPERLY RAISED IN THIS CASE.

(U) Two statutory protections also apply to the intelligence-related information, sources and methods at issue in this case, and both have been properly invoked here as well. First, Section 6 of the National Security Agency Act of 1959, Pub. L. No. 86-36, § 6, 73 Stat. 63, 64, codified at 50 U.S.C. § 402 note, provides:

> [N]othing in this Act or any other law . . . shall be construed to require the disclosure of the organization or any function of the National Security Agency, of any information with respect to the activities thereof, or of the names, titles, salaries, or number of persons employed by such agency.

Id. Section 6 reflects a "congressional judgment that in order to preserve national security, information elucidating the subjects specified ought to be safe from forced exposure." *The Founding Church of Scientology of Washington, D.C., Inc. v. Nat'l Security Agency*, 610 F.2d 824, 828 (D.C. Cir. 1979); *accord Hayden v. Nat'l Security Agency,* 608 F.2d 1381, 1389 (D.C. Cir. 1979). In enacting Section 6, Congress was "fully aware of the 'unique and sensitive' activities of the [NSA] which require 'extreme security measures.'" *Hayden*, 608 F.2d at 1390 (citing legislative history). Thus, "[t]he protection afforded by Section 6 is, by its very terms, absolute. If a document is covered by Section 6, NSA is entitled to withhold it . . . ." *Linder v. Nat'l Security Agency,* 94 F.3d 693, 698 (D.C. Cir. 1996).

(U) The second applicable statute is Section 102A(i)(1) of the Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, 118 Stat. 3638 (Dec. 17, 2004), codified at 50 U.S.C. § 403-1(i)(1). This statute requires the Director of National Intelligence to protect intelligence sources and methods from unauthorized disclosure. The authority to protect intelligence sources and methods from disclosure is rooted in the "practical necessities of modern intelligence gathering," *Fitzgibbon v. CIA,* 911 F.2d 755, 761 (D.C. Cir. 1990), and has been described by the Supreme Court as both "sweeping," *CIA v. Sims,* 471 U.S. at 169, and "wideranging." *Snepp v. United States,* 444 U.S. 507, 509 (1980). Sources and methods constitute "the heart of all intelligence operations," *Sims,* 471 U.S. at 167, and "[i]t is the responsibility of the [intelligence community], not that of the judiciary to weigh the variety of complex and subtle factors in determining whether disclosure of information may lead to an unacceptable risk of compromising the . . . intelligence-gathering process." *Id.* at 180.

(U) These statutory privileges have been properly asserted as to any intelligence-related information, sources and methods implicated by Plaintiffs' claims, and the information covered by these privilege claims are at least co-extensive with the assertion of the state secrets privilege by the DNI. *See* Public McConnell Decl. ¶ 10; Public Alexander Decl. ¶ 12. Moreover, these privileges reinforce the conclusion that the state secrets privilege requires dismissal here, and provide an additional, independent basis for that conclusion. The fact that intelligence sources and methods, as well as information concerning NSA activities, are subject to express statutory prohibitions on disclosure underscores that the need to protect such information does not reflect solely a policy judgment by the Executive Branch, but the judgment of Congress as well.

(U) Since the Court's decision in *Hepting*, Section 6 of the National Security Act has been applied in a FOIA context to information concerning the Terrorist Surveillance Program. *See People for the American Way Foundation v. National Security Agency/Central Security Service*, 462 F. Supp. 2d 21 (D.D.C. 2006). In *PFAW*, the court applied Section 6 to preclude disclosure under FOIA of several categories of information related to the TSP, including the number of individuals subject to surveillance under the program, the number of communications intercepted, the identity of individuals targeted and, in particular, information that would confirm or deny whether the plaintiffs in that case had been subject to TSP surveillance—the very kind of information at issue in this case. *See id.* at 29. The court agreed that the NSA had put forward a rational explanation as to why this information should be upheld under Section 6, including that it would reveal information about NSA's success or lack of success under the TSP, as well as information about the U.S. intelligence communities capabilities, priorities, and activities. *See id.* The court also agreed that confirmation by NSA that a particular person's activities are not of a foreign intelligence interest or that NSA is unsuccessful in collecting foreign intelligence information on their activities "would allow our adversaries to accumulate information and draw conclusions about NSA's technical capabilities, sources, and methods." *See id.*

(U) The court in *PFAW* also held that Section 6 of the National Security Act does not require NSA to demonstrate what harm might result from disclosure of its activities, since "'Congress has already, in enacting the statute, decided that disclosure of NSA activities is potential harmful." *See PFAW*, 462 F. Supp. 2d at 30 (quoting *Hayden*, 608 F.2d at 1390). Finally, the court in *PFAW* rejected the contention that, because the legality of the TSP is at issue, Section 6 does not apply to protect information about NSA activities. The court held:

> Whether the TSP, one of the NSA's many SIGINT programs involving the collection of electronic communications, is ultimately determined to be unlawful, its potential illegality cannot be used to evade the "unequivocal[]" language of Section 6 which "prohibit[s] the disclosure of information relating to the NSA's functions and activities . . ."

PFAW, 462 F. Supp. 2d at 31 (quoting *Linder*, 94 F.3d at 696).[28]

---

[28] **(U)** The Court in *PFAW* also agreed that the TSP information at issue in that case was protected by the DNI's statutory privilege under 50 U.S.C. 403-1(i)(1). *See* 462 F. Supp. 2d at

(U) The Court in *Hepting* essentially disregarded the Government's statutory privilege assertions. The Court observed that "[n]either of these provisions by their terms requires the court to dismiss this action . . ." *Hepting*, 439 F. Supp. 2d at 998. That is true, but beside the point. A statutory privilege bars the disclosure of information; the consequences of that Congressional mandate are then determined in whatever proceeding the information is sought. Here, the information that Congress has barred from disclosure is central to adjudication of the case from the outset. As with the state secrets privilege, the Court's decision in *Hepting* to "determine step-by-step whether the privilege will prevent plaintiffs from discovering particular evidence," amounted to a non-decision on the substance of the statutory and state secrets privilege assertions. If, as is the case here, certain information is subject to the privilege, and if that information must be excluded under an executive privilege and by statutory law, and if as a result the case cannot proceed without that evidence, then there are no grounds for further proceedings.

[REDACTED TEXT]

(U) CONCLUSION

(U) For the foregoing reasons, the Court should:

1. Uphold the United States' assertion of the military and state secrets privilege and exclude from this case the information identified in the Declarations of J. Michael McConnell, Director of National Intelligence, and Lt. Gen. Keith B. Alexander, Director of the National Security Agency; and

2. Dismiss this action or enter summary judgment for the United States because adjudication of Plaintiffs' claims requires the disclosure of state secrets and, thus, risks exceptionally grave harm to the national security of the United States.

---

31 n.8.

Respectfully submitted,

PETER D. KEISLER
Assistant Attorney General

CARL J. NICHOLS
Deputy Assistant Attorney General

JOSEPH H. HUNT
Director, Federal Programs Branch

s/ Anthony J. Coppolino
ANTHONY J. COPPOLINO
Special Litigation Counsel
tony.coppolino@usdoj.gov

s/ Andrew H. Tannenbaum
ANDREW H. TANNENBAUM
Trial Attorney
andrew.tannenbaum@usdoj.gov
U.S. Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Avenue, NW
Washington, D.C. 20001
Phone: (202) 514-4782/(202) 514-4263
Fax: (202) 616-8460/(202) 616-8202

Attorneys for United States of America

DATED: April 20, 2007